PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Information System for Security (DISS)
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	1640
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI 007-000000594

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 24 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. 3/29/16

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number	3206-0032
Enter Expiration Date	March 31, 2017

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; E.O. 12968, Access to Classified Information; E.O. 12333 United States Intelligence Activities; E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 13467 Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoD Directive (DoDD) 5205.16, DoD Insider Threat Program; DoDD 1145.02E, United States Military Entrance Processing Command (USMEPCOM); DoD 5200.2-R, DoD Personnel Security Program; DoD Manual 5105.21, Volume 1, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security; DoDI 1304.26, Qualification Standards for Enlistment, Appointment, and Induction; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for

Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

DISS is a DoD enterprise information system for personnel security, providing a common, comprehensive medium to request, record, document, and identify personnel security actions within the Department including: determinations of eligibility and access to classified or national security information, suitability and/or fitness for employment, and HSPD-12 determination for Personal Identity Verification (PIV) to access government facilities and systems, submitting adverse information, verification of investigation and/or adjudicative status, support of continuous evaluation and insider threat detection, prevention, and mitigation activities.

DISS consists of two applications, the Case Adjudication Tracking system (CATS) and the Joint Verification System (JVS). CATS is used by the DoD Adjudicative Community for the purpose of recording eligibility determinations. JVS is used by DoD Security Managers and Industry Facility Security Officers for the purpose of verifying eligibility, recording access determinations, submitting incidents for subsequent adjudication, and visit requests from the field (worldwide).

These records may also be used as a management tool for statistical analyses, tracking, reporting, evaluating program effectiveness, and conducting research.

The types of personal information being collected includes: Name(s); Social Security Number; DoD ID Number; Personal Contact Information; Demographic information and information relating to security clearance eligibility.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Risks include unauthorized access to records or the improper handling, transmission or use of records by those authorized access to the records contained within DISS, which could result in personal or professional harm to an individual.

Access to personal information within DISS is restricted to those who have an established need-to-know in the performance of their official duties, who are appropriately screened, investigated and determined to be eligible for access. Access to personal information is further restricted by the use of Personal Identity Verification (PIV) cards for JVS and CATS. Physical entry is restricted by the use of locks, guards and administrative procedures.

All individuals granted access to these records have completed annual Privacy Act and Information Assurance training.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Office of the Secretary of Defense (OSD); Under Secretary of Defense for Intelligence (USD(I)); Under Secretary of Defense for Acquisition, Technology and Logistics (AT&L); Washington Headquarters Services (WHS); Defense Security Services (DSS); Joint Chiefs of Staff (JCS)

☒ **Other DoD Components.**

Specify. U.S. Army; U.S. Air Force; U.S. Navy; U.S. Marine Corps; and Guard/Reserve Components

☒ **Other Federal Agencies.**

Specify. U.S. Citizenship and Immigration Services; Office of Personnel Management; Federal Agencies that have employees, to include Contractors, eligible for security clearances and/or access to classified information.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Contractors with an active Facility Clearance and employees who are eligible to have a security clearance and/or access to classified national security information following National Industrial Security Program Operating Manual (NISPOM) regulations.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Information provided by individuals for a security clearance is voluntary. However, the Department may not be able to complete an investigation, or complete it in a timely manner, if the individual does not provide the necessary information.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

By completing the SF 85, SF 85P and SF 86, individuals are consenting to the specific uses of their PII.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

Privacy Act Statement is provided at initiation of investigation (SF 85, SF 85P and SF 86)